SPYWOLF

Security Audit Report

Completed on

September 5, 2023

OVERVIEW

This audit has been prepared for **Scorch** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

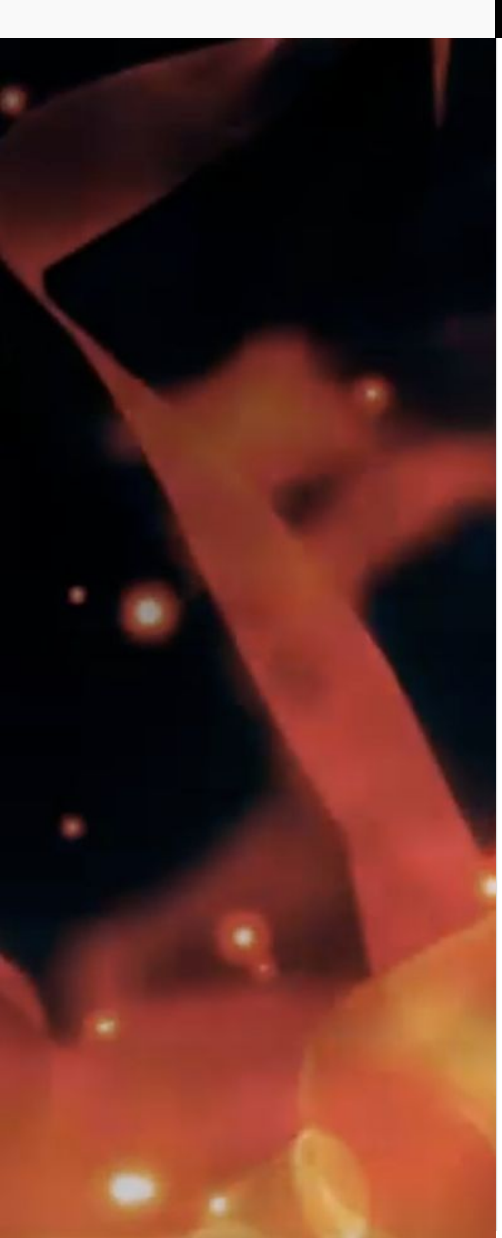
- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

Scorch



PROJECT DESCRIPTION

Website is under construction

Scorch is a special burn function project built on ERC-20 network which has taken token burning to whole new level. New kind of tokenomics helps project propell to new levels.

Scorch is a unique feature that enables token holders to burn their tokens and receive ETH in return, all while enjoying the benefits of tax-free transactions. This function offers users a convenient way to convert their tokens into a different cryptocurrency without the burden of taxes that are typically imposed on such transactions.

Release Date: Presale starts in September, 2023

Category: Token

CONTRACT INFO

Token Name
Scorch

Symbol
OTC

Contract Address
0xA3D0e72c8A2fE9127A77412BF34bEe5e4945bd49

Network
Ethereum

Language
Solidity

Deployment Date
Sep 02, 2023

Contract Type
Token with fees

Total Supply
10,000,000

Status
Not launched

TAXES

Buy Tax
4%

Sell Tax
4%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	4
Uniq Senders	3
Uniq Receivers	4
Total Amount	27431680.000000004 OTC
Median Transfer Amount	10000000 OTC
Average Transfer Amount	6857920.000000001 OTC
First transfer date	2023-09-02
Last transfer date	2023-09-04
Days token transferred	3

SMART CONTRACT STATS

Calls Count	10
External calls	6
Internal calls	4
Transactions count	7
Uniq Callers	3
Days contract called	3
Last transaction time	2023-09-04 09:21:35 UTC
Created	2023-09-02 18:37:35 UTC
Create TX	0x4aede386bb071f1602e189d78b239613bc656848bfa7bada3020df20a5ff0a3e
Creator	0xf23dd54aea42458e430b53477e9b38719fd0cc9a

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ Medium Risk

Owner can change autoswap settings.
When minimumTokensBeforeSwap is set to 0 and swapAndLiquifyEnabled is set to true and swapAndLiquifyByLimitOnly is set to true, contract will halt on sell and selling will fail.

```
function setNumTokensBeforeSwap(uint256 newLimit) external onlyOwner {
    minimumTokensBeforeSwap =  (newLimit * totalSupply()) / 10000;
}

function setSwapAndLiquifyEnabled(bool _enabled) public onlyOwner {
    swapAndLiquifyEnabled = _enabled;
    emit SwapAndLiquifyEnabledUpdated(_enabled);
}

function setSwapAndLiquifyByLimitOnly(bool newValue) public onlyOwner {
    swapAndLiquifyByLimitOnly = newValue;
}

function _transfer(
address sender,
address recipient,
uint256 amount
) internal virtual {
require(sender != address(0), "ERC20: transfer from the zero address");
require(recipient != address(0), "ERC20: transfer to the zero address");
.........................
uint256 contractTokenBalance = balanceOf(address(this));
bool overMinimumTokenBalance = contractTokenBalance >=
    minimumTokensBeforeSwap;

if (
    overMinimumTokenBalance &&
    !inSwapAndLiquify &&
    !checkMarketPair[sender] &&
    swapAndLiquifyEnabled
) {
    if (swapAndLiquifyByLimitOnly)
        contractTokenBalance = minimumTokensBeforeSwap;
    swapAndLiquify(contractTokenBalance);
}
.........................
}
```

- Recommendation:
  - minimumTokensBeforeSwap’s value should be always above 0

Informational

Owner can set buy/sell fees up to 5%.
Combined buy+sell = 10%.
When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make.
Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.

```
function setBuyFee(
    uint256 newDevTax,
    uint256 newBurnTax
) external onlyOwner {
    _buyDevFees = newDevTax;
    _buyBurnFees = newBurnTax;

    _totalTaxIfBuying = _buyDevFees.add(_buyBurnFees);
    require(
        _totalTaxIfBuying <= 5,
        "Total buy fees cannot be more than 5%"
    );
}

function setSellFee(
    uint256 newDevTax,
    uint256 newBurnTax
) external onlyOwner {
    _sellDevFees = newDevTax;
    _sellBurnFees = newBurnTax;

    _totalTaxIfSelling = _sellDevFees.add(_sellBurnFees);
    require(
        _totalTaxIfSelling <= 5,
        "Total sell fees cannot be more than 5%"
    );
}
```

Informational

When liquidity burn is enabled, every 1 hour 0.25% of token supply is burned from the liquidity pair and total supply.

```
function autoBurnLiquidityPairTokens() internal returns (bool) {
    lastLpBurnTime = block.timestamp;

    // get balance of liquidity pair
    uint256 liquidityPairBalance = balanceOf(uniswapPair);

    // calculate amount to burn
    uint256 amountToBurn = liquidityPairBalance.mul(percentForLPBurn).div(
        10000
    );

    // pull tokens from uniswap liquidity and burn them
    if (amountToBurn > 0) {
        _burn(uniswapPair, amountToBurn);
        totalBurned += amountToBurn;
    }

    //sync price since this is not in a swap transaction!
    IUniswapV2Pair pair = IUniswapV2Pair(uniswapPair);
    pair.sync();
    return true;
}

    function _burn(address account, uint256 amount) internal virtual {
    require(account != address(0), "ERC20: burn from the zero address");

    uint256 accountBalance = _balances[account];
    require(accountBalance >= amount, "ERC20: burn amount exceeds balance");
    unchecked {
        _balances[account] = accountBalance - amount;
    }
    _totalSupply -= amount;

    emit Transfer(account, address(0), amount);
}
```

Informational

Users can swap their tokens for eth directly from the contract.
They will receive the current eth value of their tokens (without taxes applied) and tokens will be burnt.
For this function to be used, the contract must have sufficient ETH for the trade size.

```
function scorch(uint256 amount) public returns (bool) {
    require(balanceOf(_msgSender()) >= amount, "not enough funds to burn");

    address[] memory path = new address[](2);
    path[0] = address(this);
    path[1] = uniswapV2Router.WETH();

    uint[] memory a = uniswapV2Router.getAmountsOut(amount, path);

    uint256 cap;
    if (address(this).balance <= 1 ether) {
        cap = burnSub1EthCap;
    } else {
        cap = address(this).balance / burnCapDivisor;
    }

    require(a[a.length - 1] <= cap, "amount greater than cap");
    require(
        address(this).balance >= a[a.length - 1],
        "not enough funds in contract"
    );

    transferToAddressETH(_msgSender(), a[a.length - 1]);
    _burn(_msgSender(), amount);

    totalBurnRewards += a[a.length - 1];
    totalBurned += amount;

    emit BurnedTokensForEth(_msgSender(), amount, a[a.length - 1]);
    return true;
}
```

- Recommendation:
  - Place burn functionality before transferToAddressETH to avoid reentrancy. However eth send via .transfer() relies only on 2300 gas
    Reference:: https://docs.soliditylang.org/en/latest/contracts.html#receive-ether-function

Informational

Owner can exclude address from fees.
When address is excluded from fees, the user will receive the whole amount of the bought, sold and/or transferred tokens.

```
function setcheckExcludedFromFees(
    address account,
    bool newValue
) public onlyOwner {
    checkExcludedFromFees[account] = newValue;
}
```

RECOMMENDATIONS FOR GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

Scorch

GOOD PRACTICES FOUND

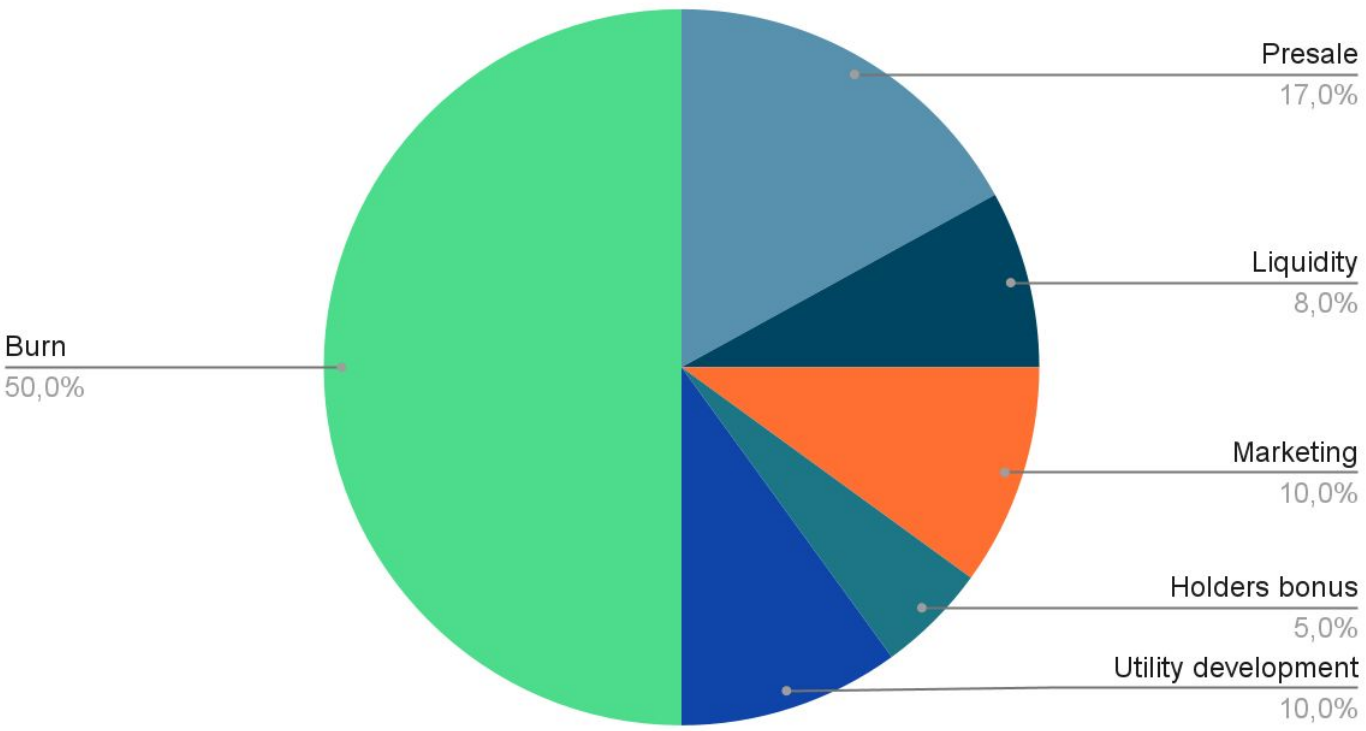
- ✔ The owner cannot mint new tokens after deployment
- ✔ The owner cannot set a transaction limit
- ✔ The smart contract utilizes "SafeMath" to prevent overflows

TOKENOMICS

The following tokenomics are based on the project's whitepaper and/or website:

- 16% - Presale
- 8% - Liquidity
- 10% - Marketing
- 50% - Burn
- 10% - Utility development
- 5% - Holders bonus

Tokens distribution



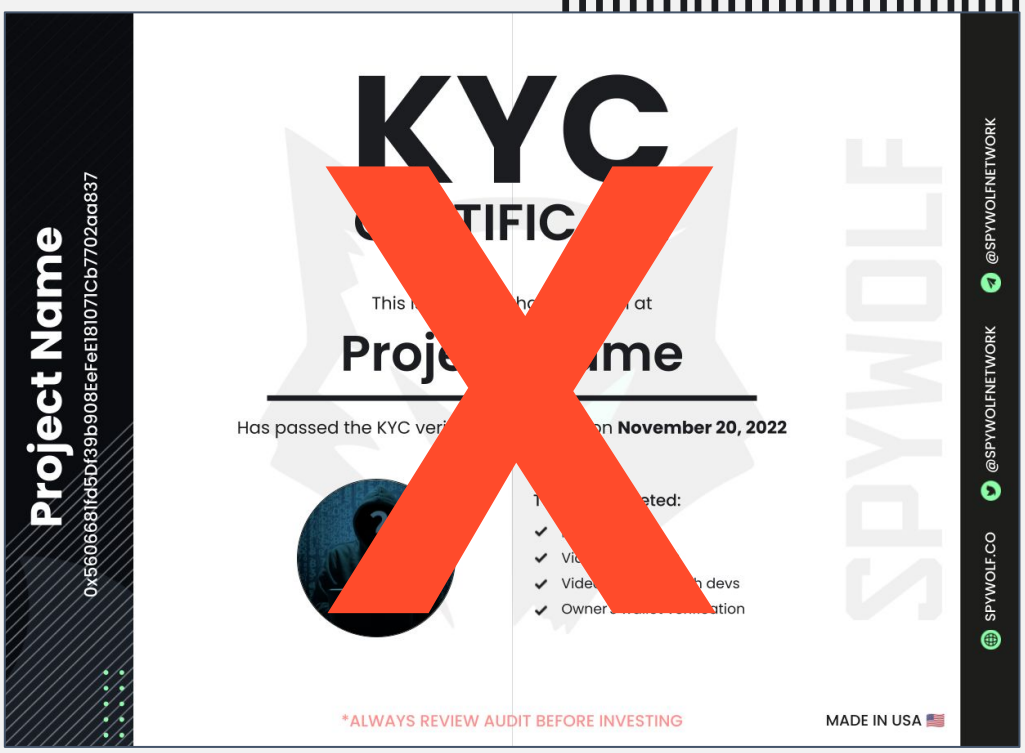
THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.



WEBSITE

Website URL
https://www.scorchcoin.com/

Domain Registry
http://www.namecheap.com

Domain Expiration
2024-09-01

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

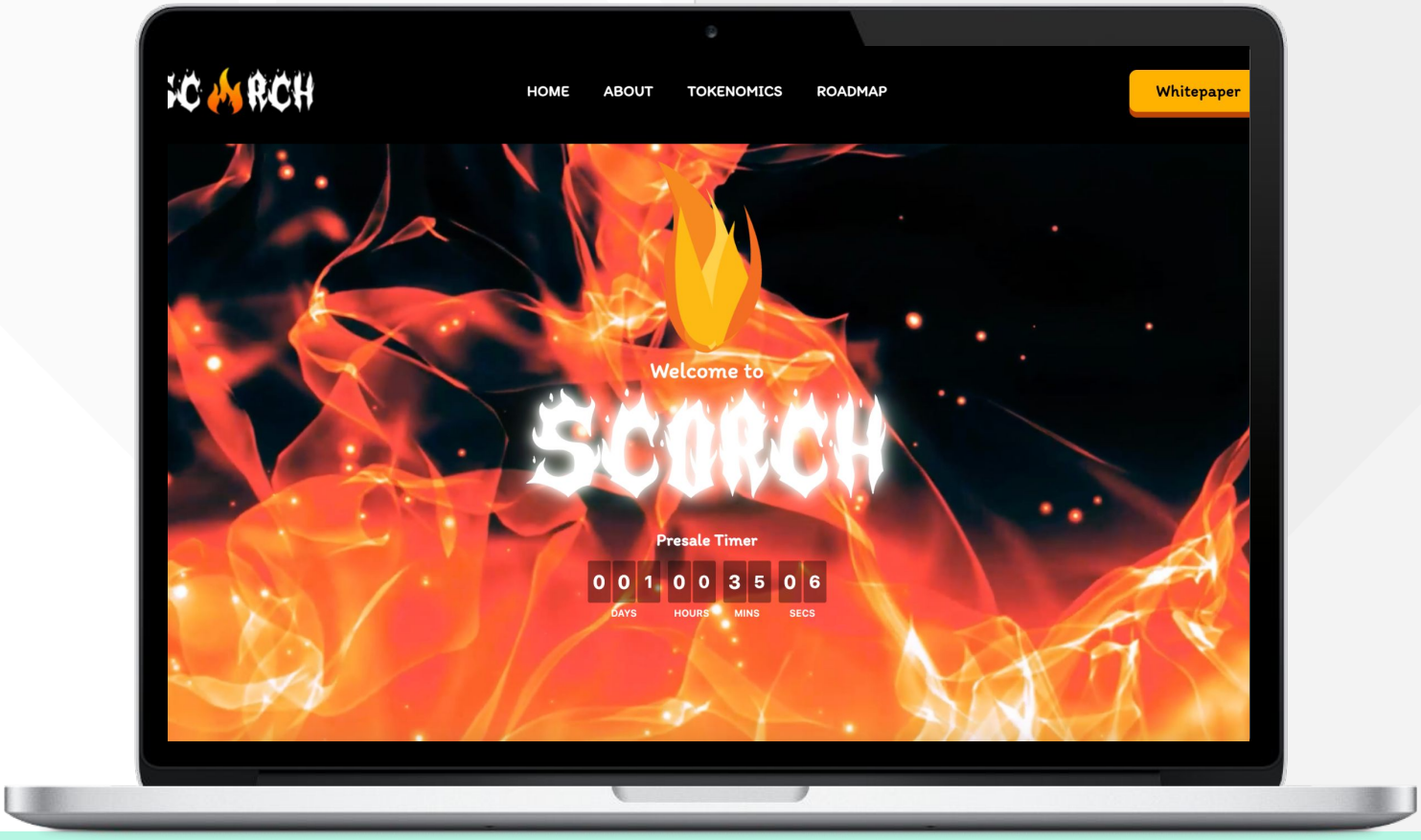
Design
Single page design with appropriate color scheme and graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found..

Whitepaper
Well written, explanatory.

Roadmap
Goals set with time frames

Mobile-friendly?
Yes



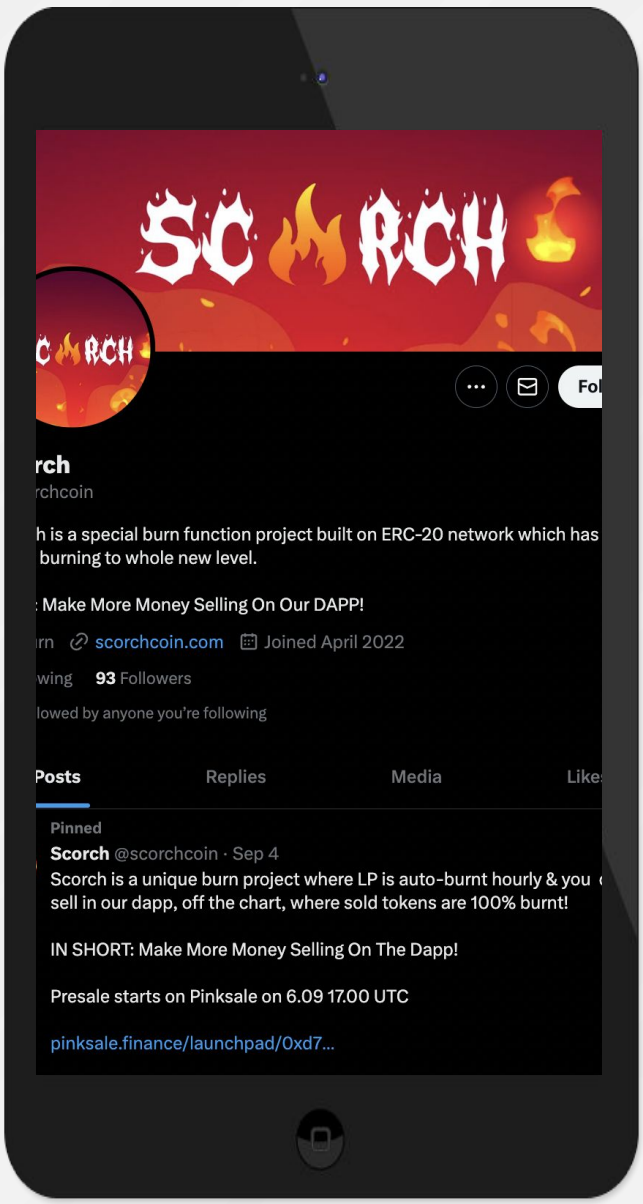
scorchcoin.com

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media pages are active



Twitter

@scorchcoin

- 60 followers
- 7 total posts
- New account
- Active

Discord

- Not available

Telegram

@scorchcoin

- 197 members
- Active members
- Active mods

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 500 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.